8635 INFORMATION AND DATA PRIVACY, SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the State's concern regarding the rise in identity theft and the need for prompt notification when security breaches occur. In accordance with New York State Education Law § 2-d, the Board hereby implements the requirements of the Commissioner's Regulations (8 NYCRR § 121 et seq.) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF).

In this regard, every use and disclosure of personally identifiable information (PII) by the district benefits students and the district (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The District also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the District will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Board of Education Policy No. 5500 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the District will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The District will comply with all such privacy provisions t6 protect the confidentiality of PH at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

The Superintendent in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII. The Board also directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the protections of “personally identifiable information” of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of “private information” under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.
- Any and all other regulations necessary and proper to implement this policy.

“Private Information” under State Technology Law §208

“Private information” is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. “Private information” does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district’s information storage or computerized data which compromises the security, confidentiality, or integrity of “private information” maintained by the district must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

• Identify and/or define the types of private information that is to be kept secure. For purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

• Include procedures to identify any breaches of security that result in the release of private information; and

• Include procedures to notify persons affected by the security breach as required by law.

Additionally, pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, the district will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the district's computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district shall be promptly reported to the Superintendent and the Board of Education.

Cross-ref: 1120, District Records
5500, Student Records
8630, Computer Resources and Data Management

Ref:

State Technology Law §§201-208

Labor Law §203-d

Education Law §2-d

8 NYCRR Part 121

Adoption date: October 7, 2009

Revised: May 5, 2010, June 17, 2020